Völkerrechtsblog
Der Blog des Arbeitskreises junger Völkerrechtswissenschaftler*innen



DIGITAL SURVEILLANCE AND CYBER ESPIONAGE SYMPOSIUM

# The surveillance you have paid for

## Cybersecurity and the Internet of Things

CHRISTIAN DJEFFAL — 5 December, 2016



Have you ever paid for surveillance measures? Not indirectly through taxes, rather directly? And have you ever installed the measures in your home? If you think that this is an absurd question, do read this blog post. It relates to four trends I would like to point out to you: the constant development of the internet of things (IoT) adds a whole new dimension to the problem of surveillance (1.). And the problem of surveillance extends far beyond surveillance by intelligence agencies (2.). These new aspects of the problem are in existence (3.). Yet, there is a significant lack of attention in the technical as well as the legal sphere (4.). This

is a governance problem transcending international, transnational and global administrative law (5).

**IoT as new dimension of surveillance**

The internet of things is not a technology but rather a vision that combines several technical trends of recent years. Its basic idea is that there is a move from an internet of computers being operated exclusively by human beings, to an internet of things in which information technology systems have a higher degree of autonomy. Computing is ubiquitous, IoT applications can observe their environment via sensors, collect data and react adequately to changes in the environment. These developments promise to make ordinary things more efficient and more user friendly. Your rubbish bin might be able to alarm the waste collection on time. Your coffee machine might sense when you wake up and prepare a coffee for you. Your heating might start to work once you are moving towards home. The number of sensors in our environment is exploding. According to a projection, the number of so called smart things will increase from 6.4 billion smart things in 2016 to over 20 billion smart things in 2020. Each of those things will have one or more sensors. This includes cameras and microphones, for example in smart TVs. This adds a whole new dimension to surveillance, as it is in many cases no longer necessary to install devices but only to hack them.

**The Democratisation of Surveillance: New Surveillance Actors**

This also means that surveillance infrastructure is no longer exclusive to intelligence agencies. Recent attacks have been conducted by paedophiles, cyber criminals or sometimes people without particular reasons. This trend could be

marked as ‘democratisation’ of surveillance due to the fact that one does not need to be a distinguished hacker to pull off such an attack. The prices for the needed software are constantly dropping and the software itself is getting more and more user-friendly. Even though it is hard to tell how many attacks and gaps are not yet public, recent reports have shown that there already is increased surveillance through IoT.

**Recent Attacks**

Almost every week a new attack or gap makes it to the news. It is very telling that the British Prime Minister has banned smart watches from cabinet meetings. The possibility to hack ‘baby cams’ received a lot of attention, especially when gaps and loopholes were used in practice. Security researchers also have warned that a smart Barbie could easily be turned into a surveillance device. On 4 November, there was coverage how the smart lighting of an office block was hacked by a drone. An insufficient password made it possible to take over 46 000 surveillance cameras that were offered to monitor homes and businesses. This is only a short glimpse into some of the recent occurrences. The list could be extended.

**Lack of Attention**

Yet, it is the general sentiment that neither businesses nor government has done enough to secure smart devices. Government agencies like the French DGCCRF or the German Ministry of Economic Affairs and Energy have highlighted the security risks of the internet of things. The FBI director James Comey recently recommended to cover up all webcams. He is quoted saying: “You do that so that people who don’t have authority don’t look at you.” While

regulators and the industry are about to take the first steps, they hardly keep pace with the development. Yet, the efforts to tackle the problem hardly match the threat level. From a technical perspective, often even simple measures such as encryption of the communication are not implemented. Regulators, legislators and interested parties have not matched what has been called for.

**Governance Problem**

The problem of increased surveillance is pertinent and can be tackled on different levels. One important way would be to address it in the context of international law. One could also think broader about frameworks such as global administrative law or transnational law. It is possible to address this problem in international law. Manufacturers can be addressed indirectly through their respective states, it would be even possible to try to provide for an international cybercrime convention in order to enhance the enforcement of the law. The existing Cybercrime Convention of the Council of Europe, for example, does not only establish a common framework of criminal law, but also aims at enhancing the cooperation of law enforcement authorities. Global administrative law would extend the scope of instruments for example to hybrid bodies or informal cooperation between governments. Transnational law would also capture collaboration between different private actors such as industry standards of several companies. International law, however, can also become relevant in a very different regard. It is mostly international institutions established by international treaties providing for the fora for multi-stakeholder exchanges on governance issues. Even if international treaties and instruments establishing

international organisations exert no direct influence on the issue, they nevertheless influence it to a great extent.

Yet, the problem of surveillance and new applications might call for a broader notion of governance. My suggestion is that individuals will play a key role in this. Their security awareness might coin the security stance in several ways. First, consumer decisions might create a demand for secure technology. Secondly, there are network effects with which consumer can potentially influence other consumers to the better or worse. The awareness existing in some groups might even be considered as a very rural form of custom that might even have a legal influence. Certain standards like the "available techniques" rely on whether a technical solution is and can be applied in practice. Thinking about the individual dimension of governance in these circumstances should not obfuscate the fact that there is not one single way to cybersecurity. Another important approach might be to stress the potential for businesses for security innovation, like French officials have done recently. Like in environmental law, regulation might turn out to spark innovation. It will take different actors such as governments, businesses and the civil society to come together and regulate cybersecurity of things. This regulation will directly affect the way I feel in my living room. If you think about it, it could affect you too.

*Dr. Christian Djeffal is project manager at the Humboldt Institute for Internet and Society and heads a team inquiring into new forms of public administration and eGovernment. He received his PhD from Humboldt University where he wrote the book "Static and Dynamic Interpretation of International Treaties" under the supervision of Georg Nolte.*

*This contribution corresponds to a presentation which has first been given at a colloquium on digital surveillance and cyber espionage, which took place from 22nd to 23rd September in Paris. Additional contributions can – in addition to those on the Völkerrechtsblog (here) – be found here and here.*

Cite this article as: ajv2016, "The surveillance you have paid for," *Völkerrechtsblog*, 5 December, 2016, http://voelkerrechtsblog.org/the-surveillance-you-have-paid-for/.

ISSN 2510-2567

**Tags:** *Cyber*, *Digitalization*, *Human Rights*



**Related**

Unilateralism ahead?
12 December, 2016
In "Digital surveillance and cyber espionage"

The dark side of digitalization
30 November, 2016
In "Digital surveillance and cyber espionage"

Whom to Obey? The incongruence of obedience to the state and its consequences for civil disobedience
1 October, 2014
In "Discussion"

PREVIOUS POST
The dark side of digitalization

NEXT POST
Der Schutz der Menschenrechte im Cyberspace durch die EMRK

## No Comment

### Leave a reply

Logged in as ajv2016. Log out?

SUBMIT COMMENT

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.